Human-Centered Network Visualizer: Visual Abstractions of Network Operations in a Tactical Environment

Christopher T. Cannon, Donald A. Pellegrino, Thomas T. Hewett, and William C. Regli
A.J. Drexel ACIN Institute
Drexel University, Philadelphia, PA, USA
Email: {ctc82, st96wym4, hewett, regli}@drexel.edu

Giovanni Oddo
US Army CERDEC CECOM C2D
Aberdeen Proving Ground, MD, USA

***Abstract*—We present visualization requirements and designs for the Human-Centered Network Visualizer (NetViz) to assist the US Army Brigade Signals Officer (S6) soldiers with their daily activities. These are based on interactions with both retired and active duty S6 soldiers. To assure information dominance, it is increasingly important that the S6 and Network Operations Group are able to obtain and provide accurate situational awareness from data received over the network. This paper addresses three challenges faced by the S6: (1) mentally integrating and correlating information from disparate tools, (2) processing and interpreting that information for a commander who may have limited technical knowledge, and (3) reducing the amount of downtime resulting from any disruption through the creation of a contingency plan. The NetViz designs abstract and unify data required by an S6 into a single view. They allow for the visualization of data to support S6 reporting during an update brief. Visual designs for "what if" scenarios and future events also facilitate planning for both the expected and the unexpected. This paper describes our interactions with S6 soldiers along with the resultant visualization enhancement based upon information provided.**

I. INTRODUCTION

The responsibility of the US Army Brigade Signals Officer (S6) is to handle all signal support matters for a unit by advising the commander and staff of the current and future state of network connectivity [1]. This responsibility can also extend outside of the unit through coordination with higher echelon signals officers and deployed task forces. To accomplish this support task, the S6 is required to rapidly correlate a series of Network Operations (NETOPS) data elements (*e.g.*, tables, graphics, pie charts, *etc.*) coming from disparate tools with regard to spectrum management, network management, information dissemination management, and information assurance. The S6 must look from tool to tool to mentally correlate the data and provide network Situational Awareness (SA) in terms understood by the commander and other members of the commander's staff whose tasks are impacted by the health of the network.

As a motivating example, consider a mobile unit communicating with a stationary unit over a satellite link. Although there are many factors important to the S6 in this scenario, one of the most relevant is how the current and future weather conditions affect the communication between units. The main objectives of the S6 in the mobile unit are to first

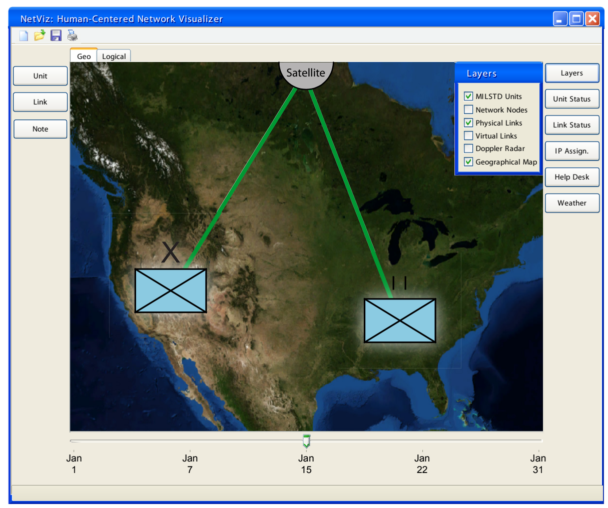

Figure 1. Human-Centered unified view.

determine the route planned by the commanding officer, predict the future weather conditions as the unit travels along the route, and finally to determine when connectivity is possible to the stationary unit based upon the predicted weather along the route. In this situation, the S6 is required to mentally correlate location, weather, and network information over time and then relay that to a commanding officer. A tool that quickly correlates and visualizes this information would relieve the S6 from the time consumption and human errors of manual calculations.

The contributions of this paper are visualization requirements and sample designs for the Human-Centered Network Visualizer (NetViz) to assist the S6 soldiers with their daily activities. These are based on our interactions with both retired and active duty S6 soldiers. The NetViz designs abstract data and information required by the S6 from various tools and allows those abstractions to be merged and/or blended into a single unified view. The proposed Unified View, shown in Figure 1, can be customized to visualize different aspects of current operations for various levels of technical skill and importance of information.

This paper is organized as follows. Section II provides an overview of current commercial off-the-shelf products, battlefield relevant device and display research, and situation awareness. Section III presents our interviews with subject

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE
Human-Centered Network Visualizer: Visual Abstractions Of Network Operations In A Tactical Environment

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
US Army CERDEC CECOM C2D,Aberdeen Proving Ground,MD,30308

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 2011 Military Communications Conference, Baltimore, MD, 07 Nov - 10 Nov 2011

14. ABSTRACT
We present visualization requirements and designs for the Human-Centered Network Visualizer (NetViz) to assist the US Army Brigade Signals Officer (S6) soldiers with their daily activities. These are based on interactions with both retired and active duty S6 soldiers. To assure information dominance, it is increasingly important that the S6 and Network Operations Group are able to obtain and provide accurate situational awareness from data received over the network. This paper addresses three challenges faced by the S6: (1) mentally integrating and correlating information from disparate tools, (2) processing and interpreting that information for a commander who may have limited technical knowledge, and (3) reducing the amount of downtime resulting from any disruption through the creation of a contingency plan. The NetViz designs abstract and unify data required by an S6 into a single view. They allow for the visualization of data to support S6 reporting during an update brief. Visual designs for ?what if? scenarios and future events also facilitate planning for both the expected and the unexpected. This paper describes our interactions with S6 soldiers along with the resultant visualization enhancement based upon information provided.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**7**	

matter experts and the requirements gathering process. Section IV presents the core NetViz visualizations including design rationale and real-world application. Finally, Section V presents conclusions and outlines future work and ongoing challenges.

II. Background

This section contains an assessment of related commercial products, applicable device and display technologies, and an overview of situation awareness and its application to the S6.

A. Assessment of Commericial Off-the-Shelf Products

Although there are many Commercial Off-The-Shelf (COTS) products related to this problem, due to space limitations of this paper we only examine the most prevalent tools in two categories: network monitoring and information visualization.

1) Network Monitoring Tools

Network monitoring tools allow the user to create, edit, and view network topologies. Examples of such tools include SNMPc [2], SolarWinds Orion [3], WhatsUpGold [4], and Microsoft System Center Operations Manager [5]. The standard visualization provided by these tools is a set of nodes that represent physical or virtual hardware, connected with lines, which represent the links that hardware uses to communicate. The user is able to drill down into a node or set of nodes to see specific attributes related to configuration and performance (*e.g.*, IP address, memory usage, disk usage, *etc*.). The information presented in this standard view can be added into the system in two ways: human input or automated collection. As the network scales and human input becomes a less viable option, these tools rely heavily on automated collection.

The Simple Network Management Protocol (SNMP), an application layer protocol designed for network management, is a common method to automatically gather data from each node on the network. The protocol works by first instantiating an agent on each managed system to expose the systems management data and report it to a central SNMP manager when requested. Network monitoring tools then process the management data from the SNMP manager and display the information to the user. This automated process initializes the network architecture and then continually requests current information from each management agent to update its current information so that the network monitoring tools can provide a real-time view of network. With this information, users can see where and how network issues are affecting the health of the network (*e.g.*, a router is offline, therefore traffic is not being delivered to its portion of the network). This information can then be plotted over time to more easily diagnose problems and ensure higher system uptime.

A weakness with most network monitoring tools is that they lack the ability to relate network information to high-level goals and objectives. A simple way to accomplish this is to overlay other information in combination with network information. This makes it easier for the user to correlate high-level information with low-level network information. For example, some network monitoring tools support geographical information. Although this is useful, the S6 has other external data sources that are as important to correlate with the network information (*e.g.*, weather, help desk tickets, military unit icons, *etc*.). Another weakness with most network monitoring tools is the amount of required knowledge and/or learning curve associated with their software. The S6 soldiers have a small window of training and then are immediately deployed. Only a small portion of the training is focused on how to operate software an S6 uses in field. An effective tool should possess intuitive navigation and assist the user in understanding complex technical events.

2) Information Visualization Tools

Information visualization tools allow the user to create, edit, and view sets of data that can be abstracted as a network. The main difference between information visualization tools and network monitoring tools is the ability to visualize any dataset that can be abstracted as a series of nodes and edges (*e.g.*, social networks, biological networks, *etc*.). Examples of such tools include Starlight [6] and Gephi [7]. The standard view presented in these tools, much like network monitoring tools, is a series of nodes connected by links. Information visualization tools typically provide robust functionality for filtering and displaying the data with a heavy focus on user customizations and the ability to support large datasets. These tools also allow for additional sources of information to be incorporated within the standard view to help the user correlate information.

Information visualization tools could better support the needs of the S6 by adding automated collection (*e.g.,* SNMP for network monitoring tools). Currently these tools rely upon the user to input an already defined dataset and work only within that static data. This presents a problem for the S6 who monitors networks that are constantly changing. Having to manually collect and enter network information on the fly would consume a great deal of time.

B. Device and Display Technologies

The touch and multi-touch interface to control electronic devices has a long history of development in the research laboratories. However, in recent years the technology to make this style of interaction with a computer widely available has moved from the laboratories into a widespread, reliable and robust technology that now has literally millions of people worldwide interacting with computing devices using the multi-touch modality. Multi-touch devices ranging from track-pads on laptop computers, table surfaces, "smart" phones, and music/video players enable a variety of communications and location-aware services.

It is within this increasingly reliable and well-supported range of capabilities and interaction styles that we have chosen to explore the possibilities for creating visualizations and visual objects that allow users to more easily integrate information across what were previously multiple displays on different devices. In particular, it is felt that the appropriate use of layers of information has great potential and offers some unique benefits in the touch/multi-touch interaction paradigm.

For example, the ability to pinch and/or expand two fingers while in contact with the touch surface and have the display contract or expand can promote an ease of navigation by eliminating cluttered controls from the screen and allow the user to drill down to find more detail on a map or allow the user to move back and re-establish a larger view of the terrain. Similarly, the appropriate layering of information allows the user to start with something like a basic terrain map, layer on top of the map the location of a variety of objects, units, or devices. Then, if needed, a weather map (*e.g.*, the Doppler radar display over the terrain of interest) can be layered on top of this. This allows creating the modern electronic equivalent of the ability to overlay several different optional transparencies to build up a more complete picture. Similarly, allowing the user to reach out, simply tap on an object twice, and have it expand into another complete picture exploits one of the strengths of hypertext and hyper-linkages, the ability to move from an overview into a more detailed sub-picture one wants to explore in greater depth. Returning to the overview or moving to other units at the same level of detail can be done equally easily.

Touch/multi-touch devices can implement many robust and reliable features. A voice recording can be captured and sent to a pre-designated set of people using a single touch. Handwriting recognition on a touch surface using either a stylus or finger is also possible. These devices are also able to utilize these features in parallel (*e.g.*, dictation of an audio recording along with note taking). Thus, the multi-touch interaction paradigm opens up many interesting potentials.

As an example, consider a large wall surface upon which is displayed a collection of sticky notes, each of which represents a key concept or idea. A group is at work organizing these ideas into a coherent pattern for planning and along a critical timeline of projected events. One member of the group recognizes an idea that is missing, writes it on a sticky note appearing on the screen of a hand held device. Once written, the note is given the flick of a finger and it slides off the screen of a device and into a holding location on the large screen where it can be viewed by all and included in the group planning. The current state of touch/multi-touch devices and software makes this scenario completely feasible.

C. *Situation Awareness*

The objective of creating new visualizations is to design tactical network visualization concepts (*i.e.*, metaphors) based on what the human eye and brain were designed to see and integrate best, quickest, and most easily so that that operator is no longer forced to use a sequential system scan to gather information. This visualization is suitable for field use and enables the S6 to easily maintain and communicate network situational awareness.

The most widely accepted general definition of Situational Awareness (SA) is that it involves "the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future [8]." Although other definitions of SA were used in a variety of studies, this definition was the most carefully scrutinized by others in the field and has withstood the test of peer evaluation.

In the case of the S6, this means that maintaining SA requires the critical elements of the network be quickly and easily recognized and that changes potentially affecting network status and well-being are easily detected. It also requires that the S6 knows and understands the meaning of the current states of the network and the effects of changes on the critical components of the network. Finally, it requires that the S6 be able to anticipate the immediate consequences of the various states of the network and predict the effects of changes in the states of the network.

Thus to help ensure that the S6 is able to maintain SA it is essential to (1) understand which factors are critical to the S6 maintaining SA; (2) integrate the representation of those critical factors in such a way that SA is maintained rather than disrupted; (3) update the representations of the critical information in real time; and (4) ensure that critical changes are observed and attended to as, or shortly after, they occur.

III. Observations and Interviews with Experts

When considering new system designs it is important to ensure that design decisions are based on the needs of the users. Through discussions with Army professionals, we collected stories and recommendations from Subject Matter Experts (SME). Stories of experiences were useful for highlighting the exceptional cases where existing technologies performed memorably. They also provided a backdrop against which needs could be understood in the larger operational picture. These experts were also asked to describe what they thought worked well and what they thought could be improved.

A. *Characterizations of the Existing Architecture*

A Science and Technology officer described the current information system landscape as typified by stove piping. This is a common characteristic of systems deployed in large organizations. It is also common when commercial packages are heavily utilized. It can be a challenge to integrate tools that were not explicitly designed to work with one another. Integration challenges can be particularly acute when tools are from a wide variety of vendors and when industry standards are note developed for the full range of information that needs to be handled.

B. *Establishing a Common Operational Picture*

A researcher from the Army Communications-Electronic Research Development and Engineering Center (CERDEC) identified a desire for a common operational picture. It was noted that automation for a simple spreadsheet-like interface that listed all of the applications, the users, and the status of each as up or down would be useful core view. A challenge of tracking policy and Access Control Lists (ACLs) was also identified. A training officer commenting on the performance of an S6 and NETOPS training event suggested that there was a need to move beyond a simple spreadsheet for the tracking of IP address and to something more formal. An S6 and his team used the analogy of a "big main control board" to express their desire for an overview of all the relevant information. A trainer remarked, "Ideally we would like a tool to monitor everything."

C. *Characterizations of the Existing Systems*

An experienced NETOPS Chief shared stories and identified a number of opportunities to provide system support. One area identified was terrain analysis in coordination with radio retransmission. A new system should aid in answering the question: Where do I setup a retransmission site? It would also be useful for a system to provide views that could be used to brief the commander. These views should support dynamic levels of detail. Getting optimal azimuth on equipment and detecting equipment with non-optimal azimuth was another area that a system could help support. The expert was able to identify cases where help desk information was best left to a dedicated system such as SharePoint. He was also able to identify cases where coordinating a help desk ticket with a device was desirable. The design consequence of this variation is that displaying help desk tickets simultaneously with the applicable machines should be user configurable. There were also cases where Wide Area Network (WAN) services may be of interest, such as the status of a mail server, and other cases where only the Local Area Network is of interest and the WAN may be a distraction.

Existing practice has a number of strengths that are important and work well. It was noted that very sophisticated naming conventions were in place. These conventions were very useful since simply obtaining the name of a machine conveyed many additional characteristics without having to look them up. Indicators that display a simple red, yellow, or green encoding of status were easy to work with and convey the status sufficiently for most cases. Discussions with additional experts revealed a need for manually setting the threshold limits on a case-by-case basis. For example, given a 10 MB/s network link, yellow might be set to 7 MB/s and red for 10 MB/s (full) load. These limits might be set differently depending on the need at the time.

Two tasks were identified that were often performed under tight time constraints, taking the system down and bringing the system up. Many discussions revealed a desire to perform manual Quality of Service by taking things off the network to reduce bandwidth consumption. The other desire was to be able to establish or recover connectivity quickly. In the scenario of limited or loss of communications, the goal is to communicate with the upper echelon for assistance. Creation of a contingency plan is seen as a good practice to facilitate establishing communications quickly, and explicit system support for contingency plans was identified as an opportunity for new system designs. Capacity planning is another good practice because during deployment, equipment may be taken beyond capacity and capacity management becomes an area of concern. An S6 and his team stressed the importance of time-critical information.

Two key needs were identified for network monitoring: (1) real-time and (2) a single system. When more than one system starts attempting to manage the SNMP traffic network efficiency is degraded. At the same time there is no additional value to be gained by having more than the authoritative network management system running. Thus, it is desirable that new designs incorporate support to detect and eliminate sources of undesirable SNMP traffic.

In one meeting with an S6 and his team between training exercises, a Major, Captain and Sergeant were able to relate a number of stories, ideas, and recommendations based on their experiences. This team thought the drill-down analogy of viewing the network provided by network monitoring tools could be very effective. Given that the team's physical work environment facilitated same-time/same-place collaboration, it was clear that table space and whiteboards would serve as useful physical tools. In addition, screen-sharing capabilities were very effective in this environment. The example of transferring a window from one laptop to another was identified as having high potential benefits. An ability to include arbitrary software, field manuals, and tactical radio into an overview was also desirable. Clearly, this is a potentially useful extension beyond use of laptops and their built-in displays.

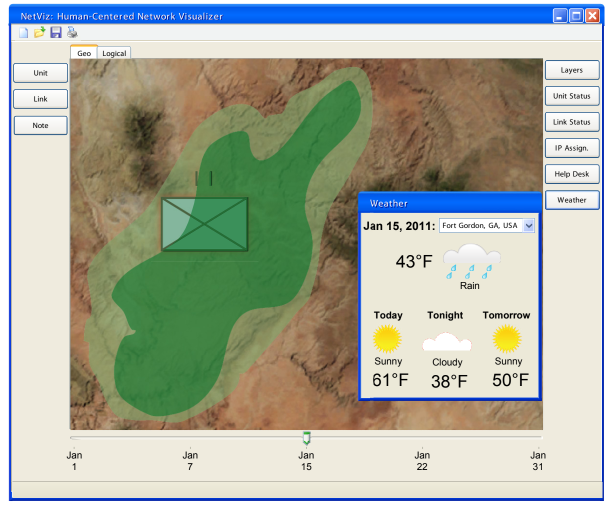

Figure 2. Weather forecast overlay.

Digital maps are of high value for many tasks and the team suggested that increased display space enhances its value. Diagrams, particularly ones implemented in Microsoft Visio [9], also played an important role. A trainer making summary recommendations for problem solving suggested; "map it out and diagram." One area where additional technological support is particularly useful is mapping between physical systems and virtual machines. Finally, weather tracking again was identified as important, not just for connectivity concerns, but also for concerns about heat and other environmental conditions that might be affecting electronic equipment.

An experienced S6 identified a number of additional considerations. Falling in on existing equipment was an activity that could lead to challenges. In this scenario, the details of the equipment may not be fully known to those who are then tasked with maintaining it. Such equipment may have configuration settings that no longer fit the current needs. For example, routers may make use of VLANS that the new staff does not know about. He also stressed the criticality of the time dimension and planning. The S6 spends significant time planning and troubleshooting. Therefore, the ability to move forward (*i.e.*, planning and modeling) and backward (*i.e.*, historical data review) are important capabilities. These are also areas of opportunity for improved system support. For example, consider the case of moving a laptop from one unit to another, and subsequently from one network to another. In this case, the laptop may need to have DNS settings reconfigured by an administrator. A forward planning tool should be able to model this change and alert the staff to a need for reconfiguration before the laptop can be redeployed. Alternatively, if a laptop is received that fails to establish connectivity, a backward historical data analysis should be able to reveal that a DNS change was made recently and thus provide the staff with a starting point for further analysis.

The most experienced of the S6 soldiers we spoke with also identified two key issues that he expected to grow in importance in the future: (1) scalability and (2) information assurance/network defense. The scalability concern corresponds with feedback received from a CERDEC researcher that scalability is becoming a big issue as the number of sensors and devices are constantly increasing. The information assurance/network defense area requires the capability to detect, isolate, and lock down an infected or compromised node. The strategy of taking down everything is not feasible. Ideally, a remote management node needs to be preserved to allow for remediation, so the lock down needs to be done carefully in these scenarios.

D. S6 Critical Factors

As a result of the cognitive task analyses to date (*e.g.*, SME interviews, questionnaires, relevant military documentation, *etc.*) discussed in this section, several critical factors were revealed in the work environment of the S6 that informs visualization and/or metaphor design decisions. These critical factors are as follows.

1. **Weather:** The performance of the network can be affected by adverse weather conditions (*e.g.*, changes in radio propagation due to water vapor). The S6 must anticipate and circumvent potential weather related issues.
2. **Terrain:** The performance of the network can be affected by elements in the environment along with the mobility of units (*e.g.*, line-of-sight propagation is not possible through a mountain). The S6 must correlate terrain and operations information with network information to ensure optimal communications.
3. **Simple Network Management Protocol (SNMP):** SNMP automatically populates information about active computing devices. This relieves the S6 from constantly having to manually enter each device initially and as the network changes.
4. **NetFlow:** The NetFlow protocol captures real-time network activity. This information allows the S6 to more precisely determine the location and time of network errors.
5. **Unit Task Organization (UTO):** The organization of units within the echelon determines the flow of information as well as the expected mobility of units. The S6 can use this information to better diagnose issues and anticipate future actions.
6. **Intrusion Detection System/Intrusion Protection System (IDS/IPS):** The network can be significantly affected by external malicious attacks. The S6 must nullify or work around these attacks to ensure network stability.
7. **MILSTD2525 Symbols:** Standardized symbols carry a massive amount of meaning that is easily transferred between different roles in a unit. The S6 must translate network information to MILSTD2525 symbols so that others can interpret the information to their needs.

IV. CANDIDATE DESIGNS

In this section, we present the mock-up visualizations along with their design rationale. Due to the space limitations of this paper, we only present a subset of the NetViz mock-up visualizations.

A. Human-Centered Unified View

The mock-up visualization, shown in Figure 1, displays the human-centered unified view, which is essential to an S6 because it shows real-time network connectivity as it relates to the units and their geographical positions. The three layers of information within this view are: (1) US Army MILSTD2525 symbology, (2) satellite network connectivity, and (3) geo-referenced unit positions. The MILSTD2525 symbols represent the military operations perspective and allow any member of the unit to relate this view to the current mission. The satellite network connectivity shows a traditional node-link diagram. The network information in this view is dynamically populated and updated by discovery protocols (*e.g.*, SNMP). The geo-referenced position layer shows geospatial information (*e.g.*, terrain models), which can be collected from geographical information systems. This view also demonstrates the layers palette, which allows the user to customize the human-centered view by overlaying mission-relevant information to suit the requirements of the user.

B. External Information and Timeline

The mock-up visualization, shown in Figure 2, displays how information overlays can correlate mission-specific information with external factors that could affect the mission. Specifically, we show how weather information in the form of a predicted forecast and Doppler radar can be correlated with mission planning. Although we only display weather information, which we have assessed to be one of the important factors that an S6 must consider, the NetViz interface allows other types of data as well. As an example, we have additional functionality in the form of buttons along the right-hand side of the NetViz interface. These tools allow further inspection of interface elements and are as follows:

1. **Layers**: The layers tool allows the user to customize the visibility and order of data sources displayed on the NetViz interface.
2. **Unit Status:** The unit status tool displays information about a specific unit (*e.g.*, latitude, longitude, uptime, status of services, *etc.*).
3. **Link Status:** The link status tool displays information about a specific link between units (*e.g.*, type of link, bandwidth, latency, packet loss, *etc.*).
4. **IP Assignment:** The IP assignment tool assists the S6 in keeping track of physical nodes assigned to IP addresses as typically all IP addresses are statically assigned. It also shows graphs of network traffic over time so the S6 can better determine how an error is affecting the network.
5. **Help Desk:** The help desk tool integrates the S6's help desk ticketing system so that a ticket can be associated with the pertinent node(s).
6. **Weather:** The weather tool displays the current weather and temperature along with the predicted forecast for the next 24 hours.

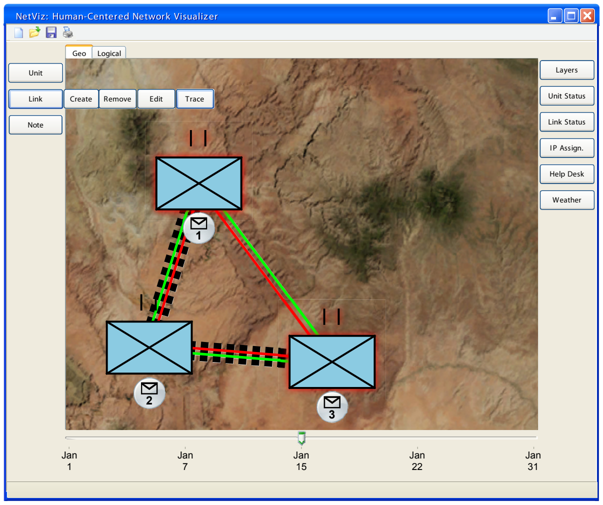

Figure 3. Network connectivity and trace between units.

The other important element in this mock-up visualization is the timeline below the main visualization area. This timeline allows the user to scrub forward or backward in time while dynamically updating the main view. Initially, as shown in Figure 2, we show the current weather and Doppler radar overlay. However, if we were to scrub backwards in time the visualization area would update the weather to the previous day's forecast. Along with updating the forecast, the unit's position and every other piece of information with historical data is updated according to the previous date that was chosen. The ability to scrub backwards in time allows the S6 to present the events that occurred during their shift at an update brief. During this brief, the S6 can simultaneously show what error occurred (*e.g.*, network outage) along with what caused that error to occur (*e.g.*, cloud coverage blocking the satellite signal). The ability to scrub forwards in time allows the S6 to effectively plan for future events and play out each possible scenario as if it were happening. As an example, consider a contingency plan that consists of a commander requesting the S6 to determine if satellite connectivity will be affected by future weather conditions. Using the future timeline functionality, the S6 scrubs forward to determine if the amount of cloud cover predicted over that period would warrant a network outage.

C. Network Connectivity and Visual Packet Trace

The mock-up visualization, shown in Figure 3, displays the network connectivity and visual packet trace functionality of the NetViz interface. We split the visualization of network connectivity into two categories: physical and virtual. Physical connections are either reliable or unreliable and shown as bold black solid or dotted lines, respectively. In Figure 3, we show the units connected over radio links, an unreliable network connection, so the links are bold dotted black lines. To visualize virtual connections we color them according the type of traffic that is transported over the virtual connections. In Figure 3, we show a solid red and green line representing the SIPRNET and NIPRNET, respectively. One item of note in Figure 3 is that there is not a physical connection between Unit One and Unit Three, yet a virtual link exists between them. This virtual link is present because Unit Two forwards traffic from Unit One to Unit Three and vice versa. If the link between Unit One and Unit Two were to go down, so would the virtual link between Unit One and Unit Three.

The other important element in Figure 3 is the visual packet trace functionality. Figure 3 shows Unit One and Unit Three as highlighted while the user clicks the Trace button. The Trace button creates a visual traceroute by appending numbered hops to each node along the path from the source to the destination. This functionality is important to the S6 for determining not only if the traffic is flowing, but also how the traffic is flowing. For example, consider the scenario were a DNS entry is improperly configured and traffic that is supposed to be going to a specific unit is in actuality going to a completely different unit. The packet trace tool provided by the NetViz interface can assist the S6 in debugging this issue and determine when the misconfigured DNS entry is properly configured.

V. CONCLUSIONS AND FUTURE WORK

This paper presented visualization requirements and designs for NetViz. These designs are based on an assessment of current COTS products, battlefield relevant device and display research, and network situation awareness. They are informed by stories and recommendations from expert signal personnel. The designs leverage technologies that are available today. They leverage human capabilities for integrating information from multiple sources visually. They can therefore help signals personnel iterate through the Military Decision Making Process faster and more thoroughly. The systems environment of the S6 makes use of many software systems and tools to provide the necessary information at the right time. The ability to use commercial tools that were developed for generalized needs and markets has many advantages, such as reduced acquisition costs and sustainable continuous improvement. A consequence of this approach however, is that data integration from multiple tools becomes a challenge. The NetViz approach focuses directly on data integration and presents designs for performing integration in the specific ways that address the specialized needs of the S6.

REFERENCES

[1] United States, "Tactical Local Area Network (LAN) Management: Field Manual 24-7," Department of US Army, Tech. Rep., 1999.
[2] "Network Management – Castle Rock Computing – SNMPc." [Online]. Available: http://www.castlerock.com
[3] "Orion Network Performance Monitor – SolarWinds." [Online]. Available: http://www.solarwinds.com/products/orion
[4] "Network Management Software | Server Monitoring | WhatsUp Gold." [Online]. Available: http://www.whatsupgold.com
[5] "System Center Operations Manager 2007 (SCOM) – Platform Monitoring." [Online]. Available: http://www.microsoft.com/systemcenter/en/us/operations-manager.aspx
[6] "PNNL: Starlight Information Visualization Technologies." [Online]. Available: http://www.starlight.pnnl.gov/
[7] "Gephi, an open source graph visualization and manipulation software." [Online]. Available: http://www.gephi.org/
[8] M.R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors: The Journal of Human Factors and Ergonomics Society*, vol. 37, no. 1, pp. 32—64, 1995.
[9] "Microsoft Visio 2010 – Microsoft Office." [Online]. Available: http://www.office.microsoft.com/en-us/visio